NEW YORK
LONDON
SINGAPORE
PHILADELPHIA
CHICAGO
WASHINGTON, DC
SAN FRANCISCO
SILICON VALLEY
SAN DIEGO
LOS ANGELES
BOSTON
HOUSTON
DALLAS
FORT WORTH
AUSTIN

DuaneMorris®

FIRM and AFFILIATE OFFICES

MICHELLE HON DONOVAN
DIRECT DIAL: +1 619 744 2219
PERSONAL FAX: +1 619 923 2967
E-MAIL: MHDonovan@duanemorris.com

www.duanemorris.com

HANOI
HO CHI MINH CITY
SHANGHAI
ATLANTA
BALTIMORE
WILMINGTON
MIAMI
BOCA RATON
PITTSBURGH
NORTH JERSEY
LAS VEGAS
SOUTH JERSEY
LAKE TAHOE
MYANMAR

ALLIANCES IN MEXICO

October 25, 2024

VIA E-MAIL

Office of the Attorney General
Attn: Data Security Incident
200 St. Paul Place
Baltimore, MD 21202

Re: Incident Notification

Dear Mr. Brown:

We are writing on behalf of our client, Data Systems Analysts, Inc. (DSA), to notify your office of a data security incident involving 54 Maryland residents.

On July 11, 2024 DSA discovered that a business email account was compromised by a threat actor in connection with a scheme to commit wire fraud. Upon discovery, DSA immediately engaged a cyber security expert who worked with its Chief Information Security Officer to investigate and remediate the situation. DSA could not rule out the possibility that the emails and attachments in the company account may have been viewed or accessed and it was not immediately clear whether any sensitive personal information was accessed in the affected account. In an abundance of caution, DSA engaged in a time-intensive review of all emails and attachments in the account. After completing this investigation, we discovered that there was a limited amount sensitive personal information. This review was completed on October 21, 2024.

Affected information varies depending on the individual and may include one or more of the following: social security number, redacted social security numbers (last 4 digits only), and passport information. At this time, we have no reason to believe the information was, or will be, misused.

DSA takes IT security, the privacy/protection of our data and the response to this incident seriously. In addition to the existing Managed Security Service Provider (MSSP) measures employed which include a Security Incident and Event Monitoring (SIEM) System, Sentinel One Extended Detection and Response (XDR) platform, Automox endpoint management and

vulnerability patching software platform, and a 24x7 manned Security Operations Center (SOC), DSA has taken additional measures to strengthen its cybersecurity posture in the wake of the aforementioned security incident, including but not limited to:

- Conducted one-on-one training for the employee whose account was compromised
- Issued notifications about the nature of the incident and associated precautions to all DSA employees
- Conducted additional detailed forensics briefings to DSA Executive Leadership
- Completed an independent, external audit of DSA's overall Information Security Management System (successful ISO 27001:2022 Recertification Audit conducted 7/30 – 8/2/2024)
- Implemented enhanced organizational password complexity measure requirements (increased from 8 character complex password to a 12 character complex passphrase) to be changed NLT every 90 days
- Implemented enhanced organizational Data Leakage Prevention (DLP) technical controls
- Reinforced security awareness topics weekly during October Cybersecurity Awareness Month
- Continued conducting internal phishing campaigns and reinforced employee phishing awareness
- Replaced and improved the DSA deployed SIEM system for better and faster detection of anomalous IT security activities
- Implementing more restrictive Multi-Factor Authentication (MFA) controls in DSA's commercial Microsoft 365 tenant.

Notice to potentially affected individuals will be mailed on October 28, 2024, along with the means to enroll in a complimentary one-year subscription for a credit monitoring and identity theft protection program. A copy of the Notice is attached.

Please contact me if you have any questions or need any additional information regarding this matter.

Very truly yours,

Michelle Hon Donovan

Michelle Hon Donovan
Partner

MHD
Attachment

Data Systems Analysts, Inc.
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

P
[redacted]

October 28, 2024

Re: Notice of Data Breach

Dear [redacted]:

First, I would like to express our appreciation for your employment relationship with Data Systems Analysts, Inc. (DSA). It is our goal to be transparent about issues as they arise. In that vein, I am writing to advise you of a recent security incident that may have compromised your personal information and the efforts we are taking to help you ensure that any personal information is protected.

What Happened
On July 1, 2024 certain business email accounts were compromised by a threat actor in connection with a scheme to commit wire fraud. Upon discovery, we immediately engaged a cyber security expert who worked with our Chief Information Security Officer to investigate and remediate the situation. It was not immediately clear whether any sensitive personal information was accessed in the affected accounts. However, after completing our investigation, we discovered that there was a limited amount sensitive personal information in these accounts.

What Information Was Involved
Based on the investigation to date, we believe that the following information about you was affected by this breach: Name, Social Security number, and date of birth. At this point, we have no direct knowledge as to whether your personal information was actually accessed or viewed by the threat actor or whether your personal information has been improperly used or that improper activity will occur. Nevertheless, in an abundance of caution, we felt that it was important to advise you of these facts and the steps you may wish to take to help protect yourself (listed below).

What We Are Doing
In response to the incident, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for twelve months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

How to Enroll For Free Credit Monitoring Services
To enroll in Credit Monitoring services at no charge, please log on to https://bfs.cyberscout.com/activate and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

What You Can Do
In addition to signing up for the free credit monitoring services, please review the enclosed *Information about Identity Theft Protection* for additional information on how to protect against identity theft and fraud.

Question About This Incident
Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern Time, Monday through Friday, excluding holidays. Please call the help line at 1-800-405-6108 and supply the fraud specialist with your unique code listed above.

While representatives should be able to provide thorough assistance and answer most of your questions, you may still feel the need to speak with DSA regarding this incident. If so, please call me at [redacted] from 9:00 a.m. to 5:00 p.m. Eastern Time, Monday through Friday.

We know this is an inconvenience and we apologize for any trouble or concern this has caused you.

Sincerely,

John Somplasky

John P. Somplasky
Chief Information Security Officer
Data Systems Analysts, Inc.

Information about Identity Theft Protection

➢ *Credit Freeze*

You may also place a security freeze on your credit reports, free of charge. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. Under federal law, you cannot be charged to place, lift, or remove a security freeze. You must place your request for a freeze with each of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com). To place a security freeze on your credit report, you may send a written request by regular, certified or overnight mail at the addresses below. You may also place a security freeze through each of the consumer reporting agencies' websites or over the phone, using the contact information below.

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

1) Full name, with middle initial and any suffixes;
2) Social Security number;
3) Date of birth (month, day, and year);
4) Current address and previous addresses for the past five (5) years;
5) Proof of current address, such as a current utility bill or telephone bill;
6) Other personal information as required by the applicable credit reporting agency;

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based upon the method of your request. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze. To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (including name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report. You may also temporarily lift a security freeze for a specified period of time rather than for a specific entity or individual, using the same contact information above. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for request made by mail) after receiving your request to lift the security freeze for those identified entities or for the specified period of time. To remove the security freeze, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for requests made by mail) after receiving your request to remove the security freeze.

➢ *Fraud Alerts*

You also have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert lasts 1-year and is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. Should you wish to place a fraud alert, please contact any one of the agencies listed below. The agency you contact will then contact the other two credit agencies.

➢ *Order Your Free Annual Credit Reports*

You are entitled under federal law to one free comprehensive disclosure of all of the information in your credit file from each of the three national credit bureaus once every 12 months. Visit www.annualcreditreport.com or by calling them toll-free at 1-877-322-8228. (Hearing impaired consumers can access their TDD service at 1-877-730-4204. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

Important Contacts

To access your credit report or implement a security freeze or fraud alert, you may contact the three major credit reporting agencies listed below.

	Access Credit Report	Security / Credit Freeze	Fraud Alert
Equifax	P.O. Box 740241 Atlanta, GA 30348-5788 1-866-349-5191 www.equifax.com	P.O. Box 105788 Atlanta, GA 30348-5788 1-800-685-1111 www.equifax.com/personal/ credit-report-services	P.O. Box 105788 Atlanta, GA 30348-5788 1-888-766-0008 www.equifax.com/personal/ credit-report-services
Experian	P.O. Box 2002 Allen, TX 75013-9701 1-866-200-6020 www.experian.com	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 www.experian.com/ freeze/center.html	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 www.experian.com/ fraud/center.html
TransUnion	P.O. Box 1000 Chester, PA 19016-1000 1-800-888-4213 www.transunion.com	P.O. Box 2000 Chester, PA 19016-2000 1-888-909-8872 www.transunion.com/ credit-freeze	P.O. Box 2000 Chester, PA 19016-2000 1-800-680-7289 www.transunion.com/fraud- victim-resource/place-fraud-alert

For More Information

You can also obtain more information from the Federal Trade Commission (FTC) about identity theft and ways to protect yourself. The FTC has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information on-line at www.ftc.gov/idtheft. The general contact information for the FTC is: Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580, (202) 326-2222.

For Residents Of	Additional Information
District of Columbia	You may also obtain information about preventing and avoiding identity theft from your state Attorney General at 400 6th Street NW, Washington, D.C. 20001, (202) 727-3400. https://oag.dc.gov/
Maryland	You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General at 200 St. Paul Place, 25th Floor, Baltimore, MD 21202, (410) 576-6491. https://www.marylandattorneygeneral.gov
New York	You may also obtain also information about preventing and avoiding identity theft from the New York Attorney General: Office of the New York State Attorney General, The Capitol, Albany NY 12224-0341, 1-800-771-7755. https://ag.ny.gov/
North Carolina	You may also obtain also information about preventing and avoiding identity theft from the North Carolina Attorney General: Consumer Protection Division 9001 Mail Service Center Raleigh, NC 27699-9001, 1-877-566-7226. https://ncdoj.gov/